REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggesstions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any oenalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
28-08-2012	Related Material	-

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Introduction to Forensics and the use of the Helix free Forensic Tool	W911NF-11-1-0174
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
	206022

6. AUTHORS	5d. PROJECT NUMBER
Michelle Maldonado, Dr. Jeff Duffany (Advisor)	
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Polytechnic University of Puerto Rico 377 Ponce De Leon Hato Rey San Juan, PR 00918 -	

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211	ARO
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)
	58924-CS-REP.10

12. DISTRIBUTION AVAILIBILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

This paper was created to complement a helix tutorial that was created as an introduction into the world of forensics. For someone who would like to get started practicing computer forensics it might be a little overwhelming. There are many different tools, and techniques. Each tool will provide different capabilities and will affect the suspect system differently. Some tools can be very expensive, but there are many tools available which are free and fairly complete. The Helix tool is very robust and free of charge.

15. SUBJECT TERMS

Electronic Data, Forensics, Cyberforensics, live system.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Alfredo Cruz
UU	UU	UU	UU		19b. TELEPHONE NUMBER
					787-622-8000

Standard Form 298 (Rev 8/98)
Prescribed by ANSI Std. Z39.18

Report Title

Introduction to Forensics and the use of the Helix free Forensic Tool

ABSTRACT

This paper was created to complement a helix tutorial that was created as an introduction into the world of forensics. For someone who would like to get started practicing computer forensics it might be a little overwhelming. There are many different tools, and techniques. Each tool will provide different capabilities and will affect the suspect system differently. Some tools can be very expensive, but there are many tools available which are free and fairly complete. The Helix tool is very robust and free of charge.

The tutorial consists of a series of laboratories. Each of the laboratories will cover a different functionality provided by the Helix tool, guiding the reader in his discovery process. The goal is to provide a simple introduction into the world of forensics and to provide the reader with not just the theory but the hands on experience that every beginner is sure to need.

Introduction to Forensics and the use of the Helix free Forensic Tool

Michelle Maldonado Rodríguez
Computer Engineering
Prof. Jeffrey L. Duffany, Ph.D.
Computer Engineering
Polytechnic University of Puerto Rico

Abstract — *This paper was created to complement a helix tutorial that was created as an introduction into the world of forensics. For someone who would like to get started practicing computer forensics it might be a little overwhelming. There are many different tools, and techniques. Each tool will provide different capabilities and will affect the suspect system differently. Some tools can be very expensive, but there are many tools available which are free and fairly complete. The Helix tool is very robust and free of charge.*

The tutorial consists of a series of laboratories. Each of the laboratories will cover a different functionality provided by the Helix tool, guiding the reader in his discovery process. The goal is to provide a simple introduction into the world of forensics and to provide the reader with not just the theory but the hands on experience that every beginner is sure to need.

Key Terms — *Electronic Data, Forensics, Cyberforensics, live system.*

INTRODUCTION

Computer forensics, also called cyberforensics, is the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

Forensic investigators typically follow a standard set of procedures: After physically isolating the computer in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the hard drive. Once the original hard drive has been copied, it is locked in a safe or other secure storage facility to maintain its pristine condition. All investigation is done on the digital copy. However there are some systems that cannot be taken offline and the investigation of a live running system may be required.

Investigators use a variety of techniques and proprietary forensic applications to examine the hard drive copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation.

Computer forensics has become its own area of scientific expertise, with accompanying coursework and certification.

Our tutorial will focus on the Helix Tool. Helix can be run as an operating system, it can be run from command line and it also has a windows GUI. Helix allows for the analysis of a live system. Many corporate systems use Windows and the Windows GUI is a perfect way to get started in practicing forensics.

In this document we will have a brief discussion of computer forensics, and its use and value in our current society; so that the need for tools such as Helix by skilled professionals is understood. We will go over the functionalities that we present in the laboratories. The laboratories were prepared so that you may familiarize yourself with the Helix tool using the Windows GUI and get started in the practice of computer forensics.

The functionalities presented in the tutorial are as follows:

- **Preview System Information:** displays some general information about the system being investigated.
- **Live Acquisition:** Acquire a "live" image of a Windows System (using dd and FTK Manager).

- **Incident Response:**
  - o **MD5 Generator:** generate the MD5 signature for any file in your system
  - o **Rootkit Revealer:** detects all rootkits published at www.rootkit.com.
  - o **Internet Explorer History Viewer:** reads all the information from the history file on your computer, and displays the list of all the URLs that you have visited in the last few days
  - o **Internet Explorer Cookie Viewer:** displays the details of all cookies that Internet Explorer
- **Scan for Pictures**: scan the system to see if there are any suspicious graphic images on the suspect system.
- **Exiting Helix**: there are several ways to exit the Helix application. Some will save your actions while others won't.

COMPUTER FORENSICS

The Internet, data systems and growing computer networks provide many opportunities for computer crimes. Computers are increasingly used to commit, enable or support crimes perpetrated against business, people and property. Computers can be used to commit the crime, may contain evidence from a crime and could be targets of crime. Understanding the role and nature of evidence that might be found, how to process a crime scene containing potential forensic evidence, and how an agency might respond to such experiences of the law enforcement community, the public sector, and the private sector in the recognition. Computer forensics is commonly defined as the process of collecting, recovering, analyzing and preserving computer related data.[1]

Investigators today are increasingly facing situations in which the traditional, widely accepted computer forensic methodology of unplugging the power to a computer and then acquiring a bit-stream image of the system hard drive via a write blocker is, simply, not a viable option. For instance, it is becoming more common for investigators to encounter servers that are critical to business operations and cannot be shut down. Investigators and incident responders are also seeing instances in which the questions they have (or are asked) cannot be answered using the contents of an imaged hard drive alone. For example, how best to handle situations involving missing children who were lured from their homes or schools via instant messages (IMs), particularly when faced with the fact that some IM applications do not write chat logs to disk, either at all or in their default configurations.

Questions such as these are not limited to law enforcement. In many cases, the best source of information or evidence is available in computer memory (network connections, contents of the IM client window, memory used by the IM client process, encryption keys and passwords, etc.). In other cases, investigators are asked whether a Trojan or some other form of malware was active on the system and whether sensitive information was copied off the system. Essentially, first responders and investigators are being asked questions regarding what activity was occurring on the system while it was live, and these questions cannot be answered when following the traditional, "purist" approach to digital forensics. Members of information technology (IT) staffs are finding anomalous or troubling traffic in their firewalls and intrusion detection system (IDS) logs, and are shutting off systems from which the traffic is originating before determining which process was responsible for the traffic. Situations such as these require that the investigator perform *live response*—collecting data from a system while it is still running. This in itself raises some issues, which we will address throughout this chapter.

Perhaps more important is that the requirement to perform some kind of live response is no longer something organizations decide to do. Instead, in some ways live response is being mandated by legislation as well as regulatory bodies (the Visa Payment Card Industry, or PCI, comes to mind). When a compromise occurs on a system, these regulatory bodies ask three basic questions:

- Was the system compromised?
- Did the compromised system contain "sensitive" data? (See the appropriate legislation or regulatory guidelines for the definition of "sensitive" data.)
- If the answer to both of the preceding questions is "yes", did the compromise of the system lead to the exposure of that sensitive data?

However, many organizations are simply unprepared for an incident, and as such, the activities of their responders can expose those organizations to greater risk than the incident itself, largely due to the fact that the "shut-the-system-off-and-wipe-it" mentality of many IT organizations does not allow for the collection of the necessary data to answer the inevitable questions. These questions invariably arise when the legal or compliance department of the organization hears about the incident, and then finds out that those questions cannot be answered.[2]

Most of the digital forensics analysis tools are intended to be specialized in a particular area of the computer forensics. That is the reason why there are a variety of specialized tools available to users. Each tool has some advantages and disadvantages, it is up to the user to find a balance between them. Most of data recovery scientists will relay on various tools to ensure a complete recovery and/or analysis. However for somebody who is only beginning to experiment with forensics the process of identifying which tools complement each other and how to use them can be daunting. That is why we chose the Helix tool. By itself it is a complete enough and simple enough tool that one might work with a variety of methods, in a time fashion without having to switch between tools in order to progress.

HELIX

Forensics toolkits probe potentially compromised systems while respecting Hippocrates's dictum, "First, do no harm." To forensically probe without altering key systems or data, the Helix tool is an excellent option.[3]

The Helix tool was developed by e-fense, Inc. as an internal tool to provide the ability to acquire forensically sound images of many types of hard drives and partitions on systems running unique setups such as RAID arrays.

Helix quickly grew to include many open source, and some closed source, tools for the forensic investigators at e-fense, it became the internal standard to image "live" systems as well as systems running RAID setups. This enabled us to easily deal with the issue in the corporate world that some systems could never be taken off-line to do a more traditional forensic acquisition.

Helix was first publicly released on 23 Nov 2003. Its popularity grew quickly, and Rob Lee started using it at SANS to teach the forensics track. Helix has been going strong ever since and has been downloaded countless times. Many Government agencies and Law Enforcement community across the globe have turned to Helix as their forensic acquisition standard due to its functionality and cost effectiveness (FREE)! The National White Collar Crime Center (NW3C) has chosen to use Helix to teach Law Enforcement Linux forensics on bootable CD's.

Helix is a work in progress and is not meant to be used by individuals without proper incident response and/or forensics training if it's being used for an actual investigation. While many complex commands are simplified with a GUI interface, it is the responsibility of the end user to know what these commands are doing so that they don't accidentally delete evidence, or if called upon to testify, they don't look like an idiot when they can't explain their actions on the witness stand.

Helix could also be used for self assurance. An individual could monitor his own systems and identify if his systems have been compromised. This would help his individual to keep his system secure by identifying if a breach has been made so that he make take the necessary steps for recovery and security.

PREVIEW SYSTEM INFORMATION

The system information screen displays some general information about the system being investigated. You can see an example of the expected screen in Figure 1.

Figure 1
System Information Main Screen

This screen provides us with basic knowledge about the system that we will be working with. Some points of interest:

- "Admin:" tells us if the current user is the administrator (good security practice to change the name of the administrator account)
- "Admin Rights" tell us of the current user has administrator privileges.
- "NIC:" is the MAC access of the network card. If this value is "000000000000" it indicates that the network card is in promiscuous mode, and could be capturing all the network traffic on the system.
- "IP:" is the current IP address – this could change if the system is set up for DHCP.
- Drives name listed with no additional information (such as A:\, E:\, and G:\ in the example above) typically indicate removable drives with no media inserted.

Clicking on the small triangle next to the Preview Icon will display the second page of information, which lists the running processes. We have an example of the screen in Figure 2. Clicking the triangle will flip the between the two pages of information.

Figure 2
System Information Secondary Screen

In addition to displaying all the running processes in memory, double-clicking on any process will provide the user the option to terminate the selected application. Care should be taken, and the investigator should be sure they are terminating the proper process. Terminating the wrong process could result in system damage and loss of forensic evidence.

Why don't we just use the built in "task manager" to display this information? If they system has been hijacked by a root kit, or some other malicious program, it is possible that the Windows Task Manager has been modified to not display the malicious code. Since Helix is running from the CD, it cannot be modified, and should be able to display all the programs currently running on the system.

Now you have some knowledge about the system that you're analyzing and the processes that are being run on it. And if there are hidden processes that are running which the owner of the system was unaware of you have been able to identify those as well.

LIVE ACQUISITION

We will cover two methods for live accusation. First "Using dd" and second is the "FTK Imager"

Using dd

(dd) stands for Disk Duplication utility. The dd utility can capture physical memory and drives.

Also, dd can image over a network. Figure 3 is an example of the live acquisition screen when using dd.

Figure 3
Live Acquisition Using dd

The source field includes a drop-down box for the investigator to select any drive in the system. The destination can be a local removable drive, network drive or a net-cat listener. The image name is the user chosen name, and the standard extension is ".dd".

The Options include:

- Attached/Shared: check this option to save the image to a local drive, or a network share.
- Net-Cat: check this option to transfer the image to a net-cat server located on the network. With this option you will need to specify the IP address and port number of the net-cat server.
- Split Image: Allows you to split the image into multiple files if the image will exceed the capacity of the storage medium. For example, if you are imaging a 10 gig hard drive, you can split the image so that it will fit on a CDROM, DVD, or FAT 32 file system, which has a4 gig file size limitation.

In the program executed successfully three files will be produced and the MD5 Hashes will match. The Audit.log file should be revised:

- Filename.dd – the image of the source disk
- filename.dd.md5 – a file containing the MD5 of the image file.

- Audit.log – a file containing the command and the output of the program.

FTK Imager

FTK Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with Access Data® Forensic Toolkit® (FTK™) is warranted. Figure 4 is an example of the live acquisition screen when using FTK Imager.

Figure 4
Live Acquisition Using FTK Imager

FTK Imager can also create perfect copies (forensic images) of computer data without making changes to the original evidence." (Access Data, 2005)According to the FTK Image Help File (Access Data, 2005), you can:

- Preview files and folders on local hard drives, floppy diskettes, Zip disks, CDs, and DVDs.
- Create forensic images of local hard drives, floppy diskettes, Zip disks, CDs, and DVDs.
- Preview the contents of forensic images stored on the local machine or on a network drive.
- Export files and folders.
- Generate hash reports for regular files and disk images (including files inside disk images).To access the FTK Imager, select the second page of the Image Acquisition page. This page will display the release notes for the current version of the tool. Click on the "Imager" to launch the actual application.

The FTK imager is a powerful and flexible tool. It can be used to examine media and images, and extracted deleted files. It has extensive information available via the Help menu or the question mark icon on the toolbar.

INCIDENT RESPONSE

We will review various tools which will help us in our need for incident response.

MD5 Generator

On the top part of the second page of the incident response option you will find the option of generating the MD5 signature for any file in your system. Figure 5 illustrates this function.

Figure 5
Second Page Incident Response Panel

MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual. MD5 is intended for use with digital signature applications, which require that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem. MD5 is currently a standard, Internet Engineering Task Force (IETF) Request for Comments (RFC) 1321. According to the standard, it is "computationally infeasible" that any two messages that have been input to the MD5 algorithm could have as the output the same message digest, or that a false message could be created through apprehension of the message digest. MD5 is the third message digest algorithm created by Rivest. All three (the others are MD2 and MD4) have similar structures, but MD2 was optimized for 8-bit machines, in comparison with the two later formulas, which are optimized for 32-bit machines. The MD5 algorithm is an extension of MD4, which the critical review found to be fast, but possibly not absolutely secure. In comparison, MD5 is not quite as fast as the MD4 algorithm, but offers much more assurance of data security.[4]

Rootkit Revealer

Rootkit Revealer is a freeware tool from SysInternals. It successfully detects all rootkits published at www.rootkit.com.

A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.

A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection.

The presence of a rootkit on a network was first documented in the early 1990s. At that time, Sun and Linux operating systems were the primary targets for a hacker looking to install a rootkit. Today, rootkits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network.

Rootkits have become more common and their sources more surprising. In late October of 2005, security expert Mark Russinovich of Sysinternals discovered that he had a rootkit on his own computer that had been installed as part of the digital rights management (DRM) component on a Sony audio CD. Experts worry that the practice may be more widespread than the public suspects and that attackers could exploit existing rootkits. "This creates opportunities for virus writers," said

Mikko Hypponen, director of AV research for Finnish firm F-Secure Corp. "These rootkits can be exploited by any malware, and when it's used this way, it's harder for firms like ours to distinguish the malicious from the legitimate."

A number of vendors, including Microsoft, F-Secure, and Sysinternals, offer applications that can detect the presence of rootkits. If a rootkit is detected, however, the only sure way to get rid of it is to completely erase the computer's hard drive and reinstall the operating system.[5]

The program will run at the level of the currently logged in user. It would be best to run this as a system administrator for more accurate results.

In order to interpret the output you can find the meaning of the description column in the sysinternals web site. The results of the scan can be saved to a file using the File/Save option. This tool is meant to find rootkits, not remove them. Depending on the nature of the investigation the detection of the rootkit needs to be documented and the system preserved for future investigation.

Internet Explorer History Viewer

Each time you type a URL in the address bar or click on a link in the Internet Explorer browser, the URL address is automatically added to the history index file. This utility reads all the information from the history file on your computer, and displays the list of all the URLs that you have visited in the last few days. It also allows you to select one or more URL addresses, and then remove them from the history file or save them into a text, HTML, or XML file. In addition, you are allowed to view the visited URL list of other user profiles on your computer, and even access the visited URL list on a remote computer, so long as you have permission to access the history folder.

Internet Explorer Cookie Viewer

IECookiesView is a small utility that displays the details of all cookies that Internet Explorer stores on your computer. In addition, it allows you to do the following actions:

- Sort the cookies list by any column you want, by clicking the column header. A second click sorts the column in descending order.
- Find a cookie in the list by specifying the name of the Web site.
- Select and delete the unwanted cookies.
- Save the cookies to a readable text file.
- Copy cookie information into the clipboard.
- Automatically refresh the cookies list when a Web site sends you a cookie.
- Display the cookies of other users and from other computers.

Many of the options that were available for the Internet Explorers URLs are available for the cookies. Delete, save, open, etc. You also have the Mozilla Cookie Viewer; it works similarly to IE cookie viewer.

SCAN FOR PICTURES

This tool allows the investigator to quickly scan the system to see if there are any suspicious graphic images on the suspect system. Many different graphic formats are recognized, and displayed as thumbnails. Double clicking on any thumbnail will open the image in the local viewer. Be advised that this application will chance the last access time on just about every file in the system, since it examines the file headers to determine if the file is graphic. Keep in mind that depending on the size of the drive, the amount of memory and the speed of the system, the scan could take a while. Use example: This allows a parole officer to preview a system for graphic images that may violate a parole. Figure 6 shows us the main scan for pictures window before the pictures have been retrieved.

Figure 6
Scan for Pictures Main Window

Figure 7
Exit Generated File Example

EXITING HELIX

There are several ways to exit the Helix application.

- File / Exit from the menu bar – This will prompt an offer to save a PDF of your transactions.

- Click on the close windows button ⊠ This will also an offer to save a PDF of your transactions.

- Right –click on the Helix icon in the system tray – This will *NOT* save your transactions.

The first to exit options will save a copy of all your transactions if you will, while the last option will not. If you choose to save the output, you will be prompted in order to determine where the file will be saved. The file should be saved on a network share or on a removable evidence collection drive to prevent any contamination of the suspect computer. The default file name is Helix_Audit_Log.pdf. Figure 7 displays an example of the file that would be generated, if the user so chose.

CONCLUSION

In our current society computer forensics have a very active and growing role. For example, we use computer forensics when investigating different types of crimes where technology could have been involved and to monitor and help protect corporate and personal computer systems.

Now that you have a better understanding of what computer forensics is and why it is used you can understand why we have a need for forensic tools like Helix. It is very important to disturb the target system as little as possible to have good, accurate, reliable results in our investigation.

Depending on the type of analysis the methodology will vary. For example, if the system can be taken offline then you would make a copy of the hard drive and work off that. In this paper we focused and a "live" analysis, meaning that the system cannot be taken offline and must be investigated while it's still running. We also focused on Windows systems because most of the corporate world has windows systems and it is very likely that this could be the system that a beginner in forensic analysis might find himself working with.

When performing a forensic investigation you will be searching hidden folders and unallocated disk space for copies of deleted, encrypted, or

damaged files. You will be documenting "finding reports" and verifying your findings in preparation for legal proceedings that involve discovery, depositions, or actual litigation, or for personal documentation in order to deal with intrusions so that you may recover, protect and strengthen your system.

Our tutorial focused on the Helix Tool. Specifically it's GUI interface and some of its simplest functionalities so that you could have a basic understanding of both the tool and how to apply basic forensic principles.

We first revised the system information (Preview System Information) so that we had basic knowledge of the system we would be working with. Depending on our system and its dependencies our research approach might vary.

We also generated a live image (Live Acquisition) of the system using two different approaches (dd and FTK Imager). This image can then be analyzed without affecting the running system.

If we suspect that our system has been compromised we might need to investigate and take action on the affected system. We have many options available, in this paper we reviewed under Incident Response the MD5 Generator (generate the MD5 signature for any file in your system), the Rootkit Revealer (detects rootkits found in the system), the Internet Explorer History Viewer (reads information from the history file on your computer and displays the list of all the URLs that have been visited in the last few days) and the Internet Explorer Cookie Viewer (displays the details of all cookies that Internet Explorer).

Something else which we covered was Scan for Pictures the option. It might not be an individual's first thought when they consider a computer forensic investigation. However it could be very important. The images found in the system could reveal a lot about the person the computer system belongs to and his personal activities, interests, and hobbies. An example presented in the paper was that pedophiles might keep digital records like pictures or video of their delinquent activities.

As we mentioned before, we must keep an accurate record of our investigation process in order to ensure that our results are reliable. Helix provides a record of everything that we have done while we have been using the tool facilitating this process for the user if he should choose to use it.

The tutorials that were prepared are but a starting point for an individual interested in forensics and the Helix tool. They guide you through the process of using a new tool while encouraging you to continue the experience through self experimentation. Working with an unknown tool can be complicated. These tutorials should make the experience simpler and help you get started on the path computer forensics.

REFERENCES

[1] Stacy , Hassel Jr., "Computer Forensics For Law Enforcement", Retrieved from www.infosecwriters.com/text_resources/pdf/Forensics_HStacy.pdf

[2] Carvey , Harlan, Windows Forensic Analysis (year 2009, pages 27-28)

[3] "Definition Rootkit", Retrieved from http://searchsecurity.techtarget.com/tip/Digital-forensics-tool-Helix-does-no-harm

[4] "Definition MD5", Retrieved from http://searchsecurity.techtarget.com/definition/MD5

[5] "Definition Rootkit", Retrieved from http://searchmidmarketsecurity.techtarget.com/definition/rootkit